1 2 3 4 5 6 7 8 9 10	JEAN SCHWARTZER (NV Bar No. 11223) Jean.schwartzer@gmail.com LAW OFFICE OF JEAN SCHWARTZER 10620 Southern Highlands Parkway, Suite 110-473 Las Vegas, Nevada 89141 Telephone: 702-979-9941 CHRISTOPHER B. INGLE (AZ Bar No. 025553) cingle@maypotenza.com MICHELLE L. MOZDZEN (AZ Bar No. 028188) mmozdzen@maypotenza.com MAY POTENZA BARAN GILLESPIE 201 North Central Avenue, 22nd Floor Phoenix, Arizona 85004 Telephone (602) 252-1900 Facsimile (602) 252-1114 Pro Hac Vice Applications Pending Attorneys for Web Presence, LLC	
12	UNITED STATES DISTRICT COURT	
13	DISTRICT OF NEVADA	
14	DISTRICT OF NEVADA	
15	DEELEV MEDIA INC. a Navada Composition	G N 2.10 02422 PEP PAI
16	REFLEX MEDIA, INC., a Nevada Corporation,	Case No.: 2:18-cv-02423-RFB-PAL
17	Plaintiff, vs.	WEB PRESENCE, LLC'S MOTION TO DISMISS PLAINTIFF'S SECOND
18		AMENDED COMPLAINT
19	DOE NO. 1, an individual d/b/a www.PredatorsAlerts.com; DOE NO. 2, an individual d/b/a www.PredatorExposed.com;	
20	ARMAN ALI, an individual d/b/a D4 SOLUTIONS BD; MARCA GLOBAL, LLC, a	
21	Colorado limited liability company d/b/a www.InternetReputation.com; WEB PRESENCE,	
22	LLC, a Nevada limited liability company d/b/a www.NetReputation.com,	
23	www.GuaranteedRemoval.com, and www.ReputationLawyers.com; and DOES 3-50,	
24	inclusive,	
25	Defendants.	
26	Defendant Web Presence, LLC ("Web Presence"), by and through counsel, hereby moves to	
27	dismiss Plaintiff Reflex Media, Inc.'s Second Amended Complaint pursuant to Rules 12(b)(1) and	

12(b)(6) of the Federal Rules of Civil Procedure. This motion is based upon the following memorandum

28

of points and authorities, the Court's entire case file, and any other briefings or oral argument this Court may entertain.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION AND ISSUES.

Web Presence is a small business located in Sarasota, Florida that offers services aimed at assisting individuals and companies with improving their online visibility, ranging from creating content to improve online reputation to search engine optimization. (See, Declaration of Bryan Mendes in Support of Defendant Web Presence, LLC's Motion to Dismiss Plaintiff's Second Amended Complaint ("Mendes Decl.") ¶ 3). As part of its services, Web Presence helps clients get information removed from websites by engaging in arms-length negotiations with the websites. Mendes Decl. ¶ 4. However, Web Presence did not have a financial or ownership interest of any kind with the websites defined in the Second Amended Complaint ("SAC") as the "Extortion Websites." Mendes Decl. ¶8. Web Presence has never paid to advertise nor authorized advertisements on the Extortion Websites. Mendes Decl. ¶¶ 6, 7. Web Presence did not create profiles on SeekingArrangement.com and has never colluded or conspired with any defendant. Mendes Decl. ¶¶ 5, 12.

When the removal of negative content is a viable option, Web Presence will contact the website where that content is hosted to determine whether it will voluntarily remove that material. If a host site is willing to remove the content, it typically charges a fee for that service. Most host sites refuse to remove content for free, regardless of the veracity of the content, in part because there are no laws requiring them to remove content at all, but also because it takes time and effort to receive, process, and approve requests, not to mention editing the html coding to remove the content at issue. Not all negative or defamatory content can be removed from the internet.

The allegations in the SAC, insofar as they pertain to Web Presence, are that two people contacted Web Presence and paid for content removal, which was done successfully. These people who contacted Web Presence did not identify themselves as SeekingArrangement members, or that there was anything unusual about their removal requests. The fact that Web Presence successfully helped these two people and removed content for them is not a basis for liability to Plaintiff, nor does it support a finding that Web Presence engaged in the data mining efforts outlined in the SAC. Even Plaintiff acknowledges the

1 abs
2 fro
3 Pla
4 mu
5 sta
6 wi
7 ("7
8 spo
9 is 6
10 par
11 wo

 absence of a direct connection between Web Presence and the Data Miners by conspicuously omitting from the SAC any allegation that Web Presence played *any* role in the alleged data mining. Instead, Plaintiff attempts to drag Web Presence into this lawsuit by relying on conclusory allegations that there must be some sort of conspiracy. Vague, unsubstantiated allegations of conspiracy are insufficient to state a claim against Web Presence. At oral argument on December 19, 2018, Plaintiff admitted that without the Doe Defendants served its entire case fails. *See* Transcript of Oral Argument Proceedings ("Transcript"), attached hereto as Exhibit 1, at p. 35:2-11. To date Plaintiff has caused Web Presence to spend more than \$100,000.00 on this case, which amount continues to grow with no end in sight, which is especially galling because Plaintiff has been unable to identify, much less serve, these other necessary parties. If Plaintiff had conducted even a cursory investigation, as required by Rule 11, *Fed.R.Civ.P.*, it would have discovered that Web Presence has no involvement with, participation in, or knowledge about the conduct at issue herein. Mendes Decl. ¶¶ 11, 12.

The longer this case has gone on, the more apparent it has become that Plaintiff's actual claims, to the extent it has any, lie against the Does or Defendant Ali, and that the only defendants that are before the Court are innocent parties that Plaintiff named as defendants because it did not first ensure it had a factual basis for its claims. The only injury Plaintiff has suffered—an alleged loss of customers resulting from the creation of decoy profiles and data mining—relates to actions allegedly done by the Doe Defendants, Defendant Ali, but not Web Presence. All of Plaintiff's allegations regarding the extortion of payments in exchange for having information removed from certain websites—the only factual allegations that relate to Web Presence at all — are a) perfectly proper activities and not tortious nor illegal and b) do not support a claim that Plaintiff has standing to assert.

This Court lacks subject matter jurisdiction because Plaintiff has failed to state a claim under the Computer Fraud and Abuse Act. Plaintiff claims federal question jurisdiction under the Computer Fraud and Abuse Act ("CFAA"), which generally prohibits computer hacking. However, Plaintiff only alleges that the Data Miners misrepresented their identities and obtained information from their users. This may be a violation of Plaintiff's terms of service, but not a CFAA violation. Since the CFAA is the only basis claimed for federal jurisdiction, and Plaintiff does not allege facts that, if proven, would constitute a violation of the CFAA, this Court lacks subject matter jurisdiction over this case in its entirety.

Plaintiff's SAC fails to remedy any of the fatal issues present in its first two complaints. The

1 2 identification and service upon Defendant Aaron Wallace is a red herring, and does nothing to resolve 3 these deficiencies in Plaintiff's case against Web Presence. In Plaintiff's Reply in Support of Motion for 4 Additional Time to Conduct Discovery to Identify Doe Defendants (Dkt. 82), and at oral argument held 5 on February 19, 2019, Plaintiff does not allege at all that Wallace directed any activities of the Data Mining Defendants. Plaintiff stated: "Reflex located one Aaron Wallace, possibly responsible for 6 7 operating at least some of the extortion websites. Mr. Wallace has in fact admitted (in a phone call) that 8 he operated a predecessor to some of the extortion websites identified in this action, but claims to have 9 divested himself from such prior to the events complained of here." (Dkt. 82). Only now, that Plaintiff's 10 case is on the verge of dismissal, does Plaintiff allege that Wallace "directed" the Data Miner defendants

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

period.

II. LEGAL ANALYSIS.

Plaintiff's claims against Web Presence must be dismissed under Rule 12(b)(6), Fed.R.Civ.P. because Plaintiff fails to state a claim against Web Presence. Because Plaintiff's Computer Fraud and Abuse Act claim fails, this Court lacks subject matter jurisdiction over Web Presence and must be dismissed under Rule 12(b)(1), Fed.R.Civ.P..

to mine data, and claims that his involvement with the Extortion Websites was during the relevant time

Α. Plaintiff's Second Amended Complaint Fails to Plead Facts Sufficient to Assert a Claim against Web Presence.

Plaintiff's SAC fails to allege any specific connection, agreement, or plan between Defendant Arman Ali and other Doe Defendants (collectively, as referred to in Plaintiff's SAC, the "Data Miner Defendants" or "Data Miners")- the individual(s) allegedly engaged in data mining and posting such data on the so-called Predator Websites - and Web Presence. All of Plaintiff's claims against Web Presence are all predicated upon its incorrect assumption that Does and Web Presence, Wallace and Web Presence, or the Data Miners and Web Presence must be involved in some sort of ill-defined conspiracy. Plaintiff does not provide any evidence of such a conspiracy, nor does it make any specific factual allegations about that conspiracy. The Data Miners and Web Presence have no relationship at all.

28

1 | v 3 | I 4 | i i 5 | a a 4 | v 9 | I 1

Plaintiff's allegations state that all information gathered by the Data Miner engaged in data mining was given to them by Plaintiff's website users directly. With that information, D4 Solutions or Doe Defendants allegedly post user information onto websites, then charge those users a fee to have their information removed from such websites (referred to in the SAC as the "Extortion Websites"). Plaintiff alleges that Web Presence pays the "Extortion Websites" to remove undesirable content. When one looks at Web Presence's actions separate and apart from Doe's or the Data Miner's alleged conduct, it becomes apparent that Web Presence is engaged in the business of public relations and reputation management, which is perfectly legal. Hundreds of other reputation management companies, such as Reputation.com LLC, do this same work on a daily basis.

In fact, Plaintiff's SAC recognizes this, as the *only* issue Plaintiff seems to have with Web Presence is that "the Removal Sites [are charged] a fee to process removals" by the Extortion Websites, and that Web Presence "profit[s] from the difference between the fee" charged to the customers seeking removal, "and the fixed fee [paid] to the Extortion Website(s)." SAC ¶ 3(d).

Even assuming that everything in the SAC is true, such conduct would not give rise to a cause of action. There is nothing illegal about a website charging for removal of content, and Plaintiff has not alleged, nor can it prove that such conduct is illegal. *See*, *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1129 (9th Cir. 2014) (holding that plaintiffs' theories of extortion for failure to remove negative user reviews unless money was paid to website were covered by website's immunity under the Communications Decency Act of 1996 ("CDA"), 47 U.S.C. § 230(c)(1)). Paid content removal happens every day and many companies engage in this exact same conduct. It is commonly called "marketing" or sometimes more widely described as "public relations." Plaintiff may not like the interplay of the First Amendment, the Communications Decency Act, and the free market, but Web Presence's conduct is neither tortious nor improper.

Web Presence's conduct would be improper only if it was in league with the Data Miners, which it is not. This is the fatal missing component of Plaintiff's SAC. At no point does Plaintiff allege what, precisely, this supposed connection is. Even after amending its complaint twice, and desperately putting screenshot after screenshot of inadmissible hearsay and gossip in front of this Court, there is still no connection between the Does and Web Presence, Wallace and Web Presence, or the Data Miners and

1 | V 2 | 2 | 2 | 3 | 4 | 6 | 5 | 2 | 6 | 2

Web Presence. The identification of Aaron Wallace fails to address this deficiency. Plaintiff does not allege that Wallace is a Data Miner. The only evidence of his involvement with any of these parties at all, is that Wallace "operated a predecessor to some of the extortion websites identified in this action, but claims to have divested himself from such prior to the events complained of here." (Dkt. 82 at p.2:25-28). Significantly, there are no allegations that Wallace is involved with Web Presence, and still no allegations that Web Presence has any connection to any of the Data Miners, or any of the other Does, who still are not here before this court.

Plaintiff alleges that Web Presence operates four websites relevant to this matter. Three of them allegedly showed up in text messages, and one appeared on two banner ads. Plaintiff produced several text messages, but there is no evidence that Web Presence sent them or arranged to have them sent. Plaintiff produced an email between Chris Hinman and an unknown individual evidencing an agreement as to price and payment for content removal services, but this evidence has no reference or connection to Seeking Arrangement. From this, Plaintiff wants the Court to infer that there must be an agreement between Web Presence and the does. However, there is no evidence of a causal link, nor does Plaintiff plead one.

Even if Web Presence had sent text messages, and paid the "Extortion Websites" to remove content, it would not be illegal unless Web Presence was in league with the Data Miners, which it is not. Plaintiff would know this if it had complied with Rule 11, which Plaintiff did not¹.

1. Standards for Pleading.

Plaintiff's SAC fails because it lack any causal connection between Web Presence's alleged acts and the harm (if any) that Plaintiff allegedly suffered. A complaint must contain a "short and plain statement of the claim showing that the pleader is entitled to relief." *Fed.R.Civ.P.* Rule 8(a)(2). A pleading that offers "labels and conclusions" or "a formulaic recitation of the elements of a cause of action will not do." Nor does a complaint suffice if it tenders "naked assertion[s]" devoid of "further

¹ Web Presence intends to move for Rule 11 sanctions against Reflex and its attorneys because they know there are no facts or law supporting their claims against Web Presence and refuse to admit it. Reflex insists on pursuing the claims anyway on the theory that someday they might find some evidence. That is not the law. Plaintiff should be required to reimburse Web Presence for that harm, because Web Presence never should have been sued in the first place.

factual enhancement." *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 1949, 173 L. Ed. 2d 868 (2009), citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007).

Even though when considering a motion to dismiss the Court generally takes all of the factual allegations in the complaint as true, the Court is "not bound to accept as true a legal conclusion couched as a factual allegation." *Iqbal*, 556 U.S. at 678 (internal quotation marks omitted)).

Heightened pleading standards apply when the claims contain averments of fraud. All of Plaintiff's claims, insofar as they relate to Web Presence, allege that Web Presence engaged in a conspiracy to defraud members of Plaintiff's website, SeekingArrangement.com. In *Kearns v. Ford Motor Co.*, the Ninth Circuit specifically held that *Fed.R.Civ.P.* Rule 9(b) requires all "averments of fraud" to be pled with particularity "irrespective of whether the substantive law at issue is state or federal," and even where "fraud is not an essential element of a claim." 567 F.3d 1120, 1124–25 (9th Cir.2009). Rule 9(b)'s heightened pleading standards apply to CLRA [Consumers Legal Remedies Act] and UCL [Unfair Competition Law] claims as well because those claims are either "grounded in fraud" or at the very least "sound in fraud." *Id*.

Under Rule 9(b), all "[a]verments of fraud must be accompanied by the who, what, when, where, and how of the misconduct charged." *Vess v. Ciba–Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir.2003) (quotation omitted). Moreover, Rule 9(b) requires plaintiffs to "state the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentation." *Edwards v. Marin Park, Inc.*, 356 F.3d 1058, 1066 (9th Cir.2004). Plaintiff's allegations against Web Presence contain no such specifics.

Furthermore, to survive a motion to dismiss, a complaint must state a plausible claim for relief. *Twombly*, 550 U.S. at 556. A claim is plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "Determining whether a complaint states a plausible claim for relief is a context-specific task that requires the reviewing court to draw on its judicial experience and common sense. But where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'show[n]'—'that the pleader is entitled to relief." *Iqbal*, 556 U.S. at 679.

13

15 16

17

18 19

20

21

22

23 24

25

26 27

28

In the context of a Rule 12 motion, while the Court may presume the truth of Plaintiff's factual allegations, it cannot presume the same about its legal conclusions. "When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief." Id. at 678–79. However, "[w]hile legal conclusions can provide the framework of a complaint, they must be supported by factual allegations." Id. at 679. In this case, Plaintiff has not alleged facts that can plausibly give rise to relief. Plaintiff does not allege who acted on behalf of Web Presence, who the other Does are, when these people supposedly talked, where that conversation happened, what they talked about, what they agreed to do, or what Web Presence did to further an illegal plan. Plaintiff merely alleges that there must be some sort of conspiracy, which is insufficient as a matter of law, and then describes Web Presence's reputation management services, which are legal unless Web Presence is in league with the Data Miners. That is the fatal missing piece. As the U.S. Supreme Court stated in *Iqbal*:

The plaintiffs in *Twombly* flatly pleaded that the defendants "ha[d] entered into a contract, combination or conspiracy to prevent competitive entry ... and ha[d] agreed not to compete with one another." The complaint also alleged that the defendants' "parallel course of conduct ... to prevent competition" and inflate prices was indicative of the unlawful agreement alleged.

The Court held the plaintiffs' complaint deficient under Rule 8. In doing so it first noted that the plaintiffs' assertion of an unlawful agreement was a "'legal conclusion'" and, as such, was not entitled to the assumption of truth. Had the Court simply credited the allegation of a conspiracy, the plaintiffs would have stated a claim for relief and been entitled to proceed perforce. The Court next addressed the "nub" of the plaintiffs' complaint—the well-pleaded, nonconclusory factual allegation of parallel behavior—to determine whether it gave rise to a "plausible suggestion of conspiracy." Acknowledging that parallel conduct was consistent with an unlawful agreement, the Court nevertheless concluded that it did not plausibly suggest an illicit accord because it was not only compatible with, but indeed was more likely explained by, lawful, unchoreographed freemarket behavior. Because the well-pleaded fact of parallel conduct, accepted as true, did not plausibly suggest an unlawful agreement, the Court held the plaintiffs' complaint must be dismissed.

Iqbal, 556 U.S. at 679–80 (internal citations omitted).

2. Plaintiff's Second Amended Complaint fails to meet these standards because it has only pleaded legal conclusions couched as facts.

16 | en | 17 | 18 | do | 19 | no

22

23

20

21

2425

2627

28

Plaintiff's SAC suffers from the same deficiencies as the *Twombly* complaint, in that it attempts to disguise legal conclusions as facts. For example, Plaintiff alleges "...the Extortion Websites and the Removal Websites have an agreement that allows the Removal Sites to remove content from the Extortion Websites in exchange for payment, with the understanding that the Extortion Websites will generate clients for the Removal Websites...." (SAC \$\\$56) but fails to identify any of the particulars of that alleged agreement with respect to Web Presence. Plaintiff alleges the "Removal Sites knew or should have known" that the "Extortion Websites planned to extort individuals" and "intended for this extortion to be committed and/or cooperated in the execution of this plan" (SAC ¶¶ 82, 90, 95, 100, 103, 110, 117, 122); and the Removal Websites "knew or should have known" about the data miners' activities (SAC ¶95, 100,) but fails to plead with any particularity how or why they should have known. Plaintiff alleges that Web Presence "participat[ed] in the Extortion Scheme as described herein," but again, fails to identify any improper conduct by Web Presence. (SAC ¶¶ 96, 106, 109). Plaintiff alleges that "Defendants conspired" and that "each and every one of the Defendants is involved in a civil conspiracy" but fails to plead specifics of this alleged conspiracy insofar as it pertains to Web Presence. (SAC ¶¶ 81, 82, 90, 100, 110, 117, 122) Each of these allegations are legal conclusions couched as factual allegations. This is not enough to survive a motion to dismiss. See *Iqbal*, 556 at 678.

To allege a plausible claim against Web Presence, Plaintiff must allege something more than the defendants must have entered into some sort of an agreement or conspiracy. Plaintiff cannot make the necessary and specific factual allegations because this agreement, or evidence does not exist. Plaintiff attempts to gloss over that deficiency by making vague, conclusory allegations, but under *Twombly* those are insufficient as a matter of law.

Plaintiff would have to simply invent allegations out of whole cloth, and even though Plaintiff recklessly named Web Presence as a defendant without any factual or legal basis for doing so, even it appears reluctant to cross the line into simply making stuff up. At the end of the day, Plaintiff cannot create a claim against Web Presence by simply alleging that it must somehow be in league with Doe or the Extortion Websites. Plaintiff would have to allege facts that plausibly suggest a conspiracy, and because it has not done so, the Court must grant Web Presence's motion to dismiss. *See Iqbal*, 556 U.S. at 678.

3. Plaintiff has not shown it is plausibly entitled to relief.

"Factual allegations must be enough to rise above the speculative level." Twombly, 550 U.S. at 555. The vast majority of Plaintiff's "factual allegations" are either "based on information and belief," which is explicitly speculative, or are factual allegations couched as legal conclusions. The only factual allegations against Web Presence are that 1) a banner ad used to appear on the Predator Websites, 2) two of Plaintiff's customers allegedly received text messages that mentioned Web Presence, but were not sent from Web Presence and that Web Presence had no knowledge of, and 3) Web Presence offers content removal services for its paying customers. The Court must determine whether those allegations give rise to a "plausible suggestion of conspiracy." *Twombly*, 550 U.S. at 565–66. They do not. Like the defendant in *Twombly*, it is far more likely that Web Presence's conduct is actually lawful, unchoreographed free-market behavior. *See id.* at 567.

Plaintiff alleges that because all defendants are involved in a conspiracy against it, and that they are all liable because it was all part of a coordinated plan. But case law states otherwise. "The conspiring defendants must also have actual knowledge that a tort is planned and concur in the tortious scheme with knowledge of its unlawful purpose." *Kidron v. Movie Acquisition Corp.*, 47 Cal.Rptr.2d 752, 758 (App. 1995); *see also Wyatt v. Union Mortgage Co.* 598 P.2d 45, 51-52 (Cal. 1979) ("a plaintiff is entitled to damages from those defendants who concurred in the tortious scheme with knowledge of its unlawful purpose"); *People v. Austin*, 23 Cal.App.4th 1596, 1607 (1994) ("without knowledge of the illegal purpose there is no basis for inferring an agreement")). "Knowledge of the planned tort must be combined with intent to aid in its commission." *Kidron*, 47 Cal.Rptr.2d at 758. "While knowledge and intent may be inferred from the nature of the acts done, the relation of the parties, the interest of the alleged conspirators, and other circumstances, conspiracies cannot be established by suspicions." *Id*.

There must be some evidence. Mere association does not make a conspiracy. There must be evidence of some participation or interest in the commission of the offense. An inference must flow logically from other facts established in the action." *Id.* (citation omitted) (internal quotation marks and citations omitted). The absence of these essential allegations is not the result of oversight. Plaintiff's conclusory attempts to impute knowledge of "agents and/or co-conspirators" are insufficient to meet the

Minc as a defendant in this case.

² Curiously, Minc Law and Aaron Minc engage in the exact same content removal conduct that Web Presence does, further attestation to the legality of the practice. Plaintiff clearly knows about this, and yet has not included Minc Law or Aaron

knowledge requirement for claims alleged against Web Presence. Plaintiff's allegations regarding agency or co-conspiracy are, on their face, conclusory in nature, and not supported by factual enhancements.

Even in the light most favorable to Plaintiff, Web Presence was not one of the defendants who knew about the relationship between Plaintiff and its customers and there are no facts to show Web Presence learned about this relationship from another defendant pursuant to an alleged scheme or conspiracy. The only allegation in the SAC that purports to meet the knowledge requirement for Plaintiff's conspiracy claim states generally that "Defendants had knowledge of [Plaintiff's] relationships with its customers because they—or their agents and/or co-conspirators—subscribed as members of SeekingArrangement.com for the purpose of mining SA Members' personal identifying information." SAC ¶ 95. (emphasis added). Plaintiff's conspiracy allegation is predicated entirely on knowledge that was allegedly gained in the course of engaging in "data mining"—an activity that Plaintiff does not allege that Web Presence has engaged in. Accordingly, the SAC does not set forth allegations that support a finding that Web Presence had actual knowledge of Plaintiff's relationships with its customers. Plaintiff instead cites a number of correspondences from Minc Law² - not Web Presence — presumably in an attempt to establish 'knowledge.' SAC ¶ 95.

Plaintiff does not allege that Web Presence communicated with any of the Doe Defendants, or Aaron Wallace, or Arman Ali in any manner whatsoever. Plaintiff does not allege that any other Defendant informed Web Presence that he planned to engage in unlawful activity. Plaintiff does not allege that Web Presence agreed to assist with that plan. Plaintiff does not describe how Web Presence allegedly assisted any of these Defendants with that plan. Plaintiff does not allege that it suffered harm as a result of anything Web Presence has done. Plaintiff does not allege that Web Presence sent these text messages, because Plaintiff knows it isn't true. Web Presence has invited Plaintiff numerous times to investigate the source of those text messages, and yet has failed to do so.

The email between Chris Hinman and an unknown individual is even less compelling. The first sentence of the email thanks the unknown individual for "reaching out to us," which conveys that the unknown individual initiated contact with Net Reputation. There are no facts linking Web Presence to

1 | th
2 | th
3 | 1
4 | al
5 | in
6 | cc
7 | ki

this case. There never were. Plaintiff makes a conclusory allegation that "[e]ach Defendants intended for this extortion to be committed and/or cooperated in the execution of this plan." SAC ¶ 81, 82, 90, 100, 110, 117, 122. Plaintiff fails to allege any actual facts in support of its these claims. Plaintiff does not allege that Web Presence communicated with Doe No. 1, Ali Arman, or Aaron Wallace, agreed to engage in unlawful conduct, intended to cause Plaintiff harm, or substantially assisted with any plan. The only connections between Web Presence and this case are some text messages, which Web Presence had no knowledge of prior to this lawsuit, and Plaintiff does not even allege that Web Presence sent the alleged text message or identify who received it.

Web Presence did not participate in, conspire, or work in concert with any of the other Defendants with regard to the complained-of conduct. Absent a SA Member informing Web Presence that they were subscribers to SA, Web Presence would have no means or reason to know their customers' use of various dating websites. Even if the unidentified customers that allegedly cancelled their SA subscriptions subsequently engaged Web Presence's services, there is no allegation or evidence that their engagement with Web Presence *caused* their cancellation of services or caused any harm to Plaintiff.

B. This Court lacks Subject Matter Jurisdiction.

Federal courts are courts of limited jurisdiction. They may only hear cases where they have subject matter jurisdiction to do so. *Bender v. Williamsport Area Sch. Dist.*, 475 U.S. 534, 541-42 (1986). There are three ways to obtain federal subject matter jurisdiction: federal question, diversity of citizenship, and pendent or supplemental jurisdiction. 28 U.S.C.A. §§ 1331-2; 1367. Under Rule 12(b)(1), *Fed.R.Civ.P.*, a defendant may move for dismissal where the court lacks subject matter jurisdiction. Additionally, any rulings or judgments entered by a court which lacks subject matter jurisdiction are invalid and unenforceable. *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 137, 127 S. Ct. 764, 777, 166 L. Ed. 2d 604 (2007).

In this case, the only basis Plaintiff claims for subject matter jurisdiction is federal question. The allegation is that the Data Miners allegedly violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. SAC at ¶ 14. In December, when Plaintiff dragged Web Presence from the state of Florida, where it is located, to the Northern District of California, where Plaintiff's counsel happens to reside, Plaintiff admitted the following when pressed by Judge Hamilton:

THE COURT: I have no idea what you are saying. Start over again. I don't know what you're saying. Is there subject matter jurisdiction under the Computer Fraud and Abuse Act, the only federal claim against these two Defendants [Web Presence and Marca]?

MR. SMITH: No. THE COURT: Okay.

MR. SMITH: It's against the Does.

THE COURT: Okay. That's all I wanted, was just a straight answer. All right.

Exhibit 1 at p. 35:2-11.

Plaintiff's claim fails because it does not allege facts that, if proven, would constitute a violation of the CFAA. The conduct described in the SAC is not hacking. Plaintiff does not allege that its data was damaged by any of the defendants, including Web Presence. Plaintiff does not allege that Web Presence demanded money to repair "damage" to Plaintiff's computer systems. Plaintiff may or may not have a breach of contract claim against the Data Miners for violating its terms of service, but even if Plaintiff does have such a claim, it still would not have a claim under the CFAA. Because the CFAA is the only basis claimed for federal subject matter jurisdiction, and because Plaintiff fails to state a claim under the CFAA, this Court lacks subject matter jurisdiction over this case in its entirety. Therefore, the Court must grant this Motion to Dismiss.

1. Plaintiff's Second Amended Complaint fails to allege conduct that violates the Federal Computer Fraud and Abuse Act.

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, is the federal statute that prohibits computer hacking, specifically prohibiting unauthorized "access to a computer...and obtains information from any protected computer." 18 U.S.C. § 1030(a)(2)(C); *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 932 (E.D. Va. 2010) ("The CFAA is a civil and criminal anti-hacking statute designed to prohibit the use of hacking techniques to gain unauthorized access to electronic data.").

As a threshold issue, it is important to understand that the CFAA "targets the unauthorized procurement or alteration of information, not its misuse or misappropriation." *U.S. v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012), quoting *Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962, 965 (D. Ariz. 2008). The CFAA "do[es] not prohibit the unauthorized disclosure or use of information, but rather unauthorized access." *International Ass'n of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F.Supp.2d

1

3 4 5

6 7 8

10

11

9

12 13

15 16

14

17

18

19 20

21 22

24

25

23

26 27

28

479, 499 (D. Md. 2005). Thus, the relevant inquiry is not how the Data Miners or the Extortion Websites used Plaintiff's customer's information, but rather on how that information was obtained in the first place.

Plaintiff complains that the Data Miners a) became a user of Plaintiff's website, b) used the website to connect with other users, which is what the website is intended to do, and c) learned information from those user-to-user contacts. That conduct does not violate the CFAA because there are no allegations of computer hacking. Setting aside the fact that Plaintiff does not even allege that anyone hacked into its systems, it is also apparent that Plaintiff's allegations do not even violate the specific portions of the CFAA cited in the Complaint. For example, in paragraph 81 Plaintiff alleges "Defendants conspired to commit and attempted to commit violations of 1030(a)(2)(C), 18 U.S.C. § 1030(a)(4), 18 U.S.C. § 1030 (a)(7)(B) and 18 U.S.C. § 1030(a)(7)(C)."

Section 1030(a)(2)(C) prohibits a person from obtaining information on a protected computer without permission. Section 1030(a)(4) prohibits a person from accessing information on a protected computer without permission for use in furthering a fraud. 1030 (a)(7)(B) prohibits a person from threatening to "obtain information from a protected computer without authorization." Section 1030(a)(7)(C) prohibits a person from demanding money "in relation to damage to a protected computer," where the person intends to commit extortion and the damage was caused to facilitate that extortion. The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). In plain English, this section prohibits so-called "ransomware" attacks where a person infects a computer with malware and then demands money to restore access to the information on the computer.

Plaintiff fails to allege that any Data Miner accessed information on a protected computer at all. The SAC make it clear that despite Plaintiff's characterization of its users' information being "stolen," all information accessed by the Data Miner was provided voluntarily by SA users. Plaintiff fails to allege that any Defendant damaged its data, programs, systems, or information, and most certainly does not allege that Web Presence damaged any of those things. For that matter, Plaintiff does not allege to have suffered any "damage," as that term is defined by the CFAA, as a result of Web Presence's conduct, or at all. Nor does Plaintiff allege that Web Presence accessed information from its users, accessed

Plaintiff's computers, demanded or requested money "in relation to" the information allegedly obtained from Plaintiff's users.

Instead, Plaintiff describes a situation where its users voluntarily gave other users personal information, and now is upset that its users were careless in their disclosure of personal information to other users who turned out to be misrepresenting their identities online.

The scope of activities that the CFAA does and does not encompass can be determined not only by the plain language of the statute, but also by looking at cases where courts have held whether certain conduct is or is not covered. Examples of situations where courts have found CFAA violations include:

- A competing truck company hacked into its competitor's website in order to gain information that would allow it to take business away from its competitor. *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930 (9th Cir. 2004).
- An ex-employee used login credentials of a current employee to gain access to former employer's computer system in order to circumvent the revocation of his access. *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016).
- Employee's installation of a program on its employer's computers that causes deletion of files would constitute a CFAA violation. *International Airport Centers, L.L.C. v. Citrin,* 440 F.3d 418 (7th Cir. 2006).

In contrast, courts have not found CFAA violations in these cases:

- Prior to leaving a company, an employee emailed documents to himself that he would use afterwards to start his own business. The court held that even though the company did not like the actions the employee took with the computer, he was not restricted from accessing the computer. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009).
- Students' use of assistant principal's name and image in creating fake social media profile did not violate the CFAA. *Matot v. CH*, 975 F.Supp.2d 1191 (D. Oreg. 2013).

In *Cvent*, supra, the court drew a distinction between a website user who stole user names and passwords in order to gain access to the data on the website, which was held to be a cognizable claim under the CFAA, and a user who misused login information that plaintiff had voluntarily provided, which was held not to be a CFAA violation. 739 F. Supp. 2d. at 933. The court reasoned that a mere allegation that a defendant "used the information [which it had been given lawful authority to access] in an inappropriate way" did not state a claim for relief. Id., quoting *State Analysis*, *Inc. v. American Financial Services*, *Assoc.*, 621 F.Supp.2d 309 (E.D.Va.2009). Many other cases have similar holdings. See e.g.

1 | 1 | 2 | 3 | 1 | 4 | 4 | 5 | 6 | 1 | 6 | 1 |

LVRC Holdings LLC 581 F.3d 1127 (9th Cir.2009); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F.Supp.2d 373, 383 (S.D.N.Y.2010); Lewis–Burke Assocs. LLC v. Widder, No. 09–CV–00302–JMF, 725 F.Supp.2d 187, 193-95, 2010 WL 2926161 at *5–*6 (D.D.C. July 28, 2010). This mirrors the situation at bar, where Plaintiff admits that it created an account for the Data Miners and provided that person with a user name and password, but now complains that the Data Miners "used the information [which it had been given lawful authority to access] in an inappropriate way."

In the SAC Plaintiff alleges that the Data Miners signed up for user accounts on its website, whereupon Plaintiff granted Defendants access to the website, and then the Data Miners obtained data from other SA users and posted it on the Predator Websites. That is insufficient to allege a violation of the CFAA because there is no hacking involved.

In previously filed motions to dismiss, there has been discussion about circumventing technological barriers, and whether or not instituting IP blocks were a revocation of access. However, in this SAC, Plaintiff included a translation of a video, allegedly of one of the Data Miners, instructing the viewer and describing the process by which these accounts are made. SAC ¶ 41. It's clear from this translation that what the Data Miner is telling the viewer to do is to sign up for accounts, interact with SA members, and convince SA members to send the Data Miners their personal photos and cell phone numbers. These are all user-to-user interactions. At the end of the day, this is the heart of Plaintiff's claim. It is not a hacking claim. The Data Miners are signing up for accounts through Plaintiff's website. Plaintiff is voluntarily giving them access to the website. and the Data Miners are interacting with other SA members to obtain information.

As explained in detail above, when analyzing the CFAA cases, the discernable rule is that if someone gets access to a website, and the website did not give them access, that is hacking. If the website voluntarily gives access, even if the access was obtained under false pretenses, that conduct is not actionable under the CFAA. *See Cvent, LVRC Holdings LLC, and Matot, supra*. The real issue is whether the behavior that Plaintiff describes in the paragraph 41 of the SAC falls within the purview of the CFAA, and it doesn't. This conduct may be actionable under other state law claims, but not under the CFAA.

As stated by the court declining to find a CFAA violation in *Werner-Masuda*, and *American Family v. Rickman*, "the gravamen of [the plaintiff's] complaint is not so much that [the defendant]

2
 3
 4

improperly accessed the information ..., but rather what she did with the information once she obtained it." 554 F.Supp.2d 766, 2008. The same is true in this situation. Had the Data Miners accessed the information and used it to connect with a "Sugar Baby" or a "Sugar Daddy," as Plaintiff and its users wished, there would be no issue. We would not be here in court today. Instead, the issue Plaintiff has is what the Data Miners did with the information AFTER he obtained it.

The Data Miners are obtaining information directly from the website, or through user—to-user contacts, and Plaintiff is not happy about what the Data Miners are doing with that information. But Plaintiff still gave him access to the website. Even if access was granted under false pretenses, the CFAA is not the appropriate claim for Plaintiff to seek relief. *See e.g.*, *Matot*, supra. Misrepresenting one's identity on a dating website is not the same as computer hacking. It happens so frequently, in fact, that Merriam-Webster Dictionary defines the term "catfishing" as a verb meaning "to deceive (someone) by creating a false personal profile online." The entirety of Plaintiff's SAC can be summed up that its users are upset that they got 'catfished' and were careless in what personal information they shared online.

If Plaintiff is not happy about what the Data Miners did with the information they obtained from other user-to-user contacts, this is not a computer hacking issue – it is a state law claim, perhaps fraudulent inducement, or a breach of the website's terms of service.

2. When Plaintiff grants users access to its website, a user providing false information to obtain access is a violation of the website's terms of service, not a violation of the Computer Fraud and Abuse Act.

When a person creates an account on a website they typically will be required to check a box indicating that they consent to the website's terms of service. Ninth Circuit courts routinely hold that checking that box forms an enforceable contract between the user and the website. *E.g. In re Facebook Biometric Info. Privacy Litig.*, 185 F.Supp.3d 1155, 1166 (N.D. Cal. 2016) (enforceable contract exists where user clicks box signaling assent to terms of use). A person may breach the contract created by these terms of service, commonly known as "clickwrap" agreements, without violating the CFAA. *E.g. Nosal*, 676 F.3d at 862-63 (violation of a website's terms of use is insufficient to state a claim under the

³ https://www.merriam-webster.com/dictionary/catfish, accessed March 12, 2019.

2 3

4

5 6

7 8

9

10

11 12

13 14

15 16

17

18 19

20

21

22

24

25

23

26

27 28

CFAA because the violation does not lessen a user's "authority" to be on the website); Facebook, Inc., v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) (same). In that situation the website would have a breach of contract claim against its user, a claim which sounds in state law.

Misrepresenting one's identity online does not result in a federal computer hacking offense. It may result in a breach of contract claim for violating a website's terms of services (see e.g., Id., Twitch Interactive, Inc. v. Johnston, 16-CV-03404-BLF, 2018 WL 1449525, at *7 (N.D. Cal. Jan. 22, 2018), Yelp Inc. v. Catron, 70 F. Supp. 3d 1082, 1099 (N.D. Cal. 2014) (citing Careau & Co. v. Sec. Pac. Bus. Credit, Inc. 222 Cal.App.3d 1371, 1388 (Cal. Ct. App. 1990) (holding that a website's terms of service is a contract)), or a fraudulent misrepresentation claim (see e.g., Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 37-39 (Minn. Ct. App. 2009)), or a negligence claim (see e.g., Draker v. Schreiber, 271 S.W.3d 318, 320-21 (Tex. App. 2008)), or a defamation claim (*Id.*). It does not result in a computer hacking claim.

When presented with the choice of proceeding under a CFAA violation, or a terms of service violation, the Ninth Circuit has held that "a website's terms of service controls what is 'authorized' and what is 'exceeding authorization'—which in turn governs whether an individual's accessing information or services on the website is criminal or not, section 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will." *United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Cal. 2009).

In Drew, a website's terms of service prohibited a member from "engaging in a multitude of activities on the website, including such conduct as 'criminal or tortious activity,' 'gambling,' 'advertising to ... any Member to buy or sell any products,' 'transmit[ting] any chain letters,' 'covering or obscuring the banner advertisements on your personal profile page,' 'disclosing your password to any third party." *Id.* at 465. The *Drew* court went on to explain that "if any violation of any term of service is held to make the access unauthorized [under the CFAA], that strategy would...render the statute incredibly overbroad." Id.

Turning now to the instant case, Plaintiff alleges that the Data Miner(s) was a user of its website Seeking Arrangement. Plaintiff does not allege actual hacking. Instead, Plaintiff merely alleges the Data Miners created an account, obtained information that Plaintiff voluntarily made available to Doe No. 1,

1 and 2 a to 3 cer 4 bre 5 exp 6 fac 7 Mi 8 rev 9 doe

and then used that information in a manner that Plaintiff finds objectionable. At most, Plaintiff may have a terms of service breach of contract claim against the Data Miners, although it is difficult to say for certain because Plaintiff does not specify what its terms of service are or how the Data Miners may have breached them. For that matter Plaintiff does not allege a breach of contract claim at all, which, as explained above, is improper and overbroad. *Id.* What is clear, however, is that Plaintiff does not allege facts that, if proven, would violate the CFAA. Plaintiff alleges that it sent an email telling the Data Miners that it was not authorized to use the website, but this, again, is inadequate under the CFAA to revoke access – no technological barrier was implemented to restrict access to the Data Miners. Plaintiff does not allege that anyone hacked into its computer systems, circumvented its safeguards, or exceeded the scope of authorized access in a way that could be found to violate the CFAA.

Plaintiff's proposed interpretation of the CFAA, that individuals who misrepresent their identity online should be guilty of a federal crime, is inconsistent with the intended purpose of the CFAA, and inconsistent with case law. The Ninth Circuit, in considering what conduct constitutes unauthorized access under the CFAA, "cautioned against an overbroad interpretation that would 'expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer,' thereby "mak[ing] criminals of large groups of people who would have little reason to suspect they are committing a federal crime." *Nosal I*, 676 F.3d at 859. *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1110 (N.D. Cal. 2017). While many people may not appreciate being 'catfished' on dating websites, liability is appropriately limited to actions alleging a violation of the terms of service or misrepresentation claims, but not federal computer hacking claims.

Because the SAC does not allege facts that, if proven, would constitute a violation of the CFAA, that cause of action must be dismissed. And since the CFAA is the only basis for subject matter jurisdiction, this Court lacks jurisdiction over the entire case. Because the Court lacks subject matter jurisdiction, it must grant Web Presence's motion to dismiss. Rule 12(b)(1), Fed.R.Civ.P.

C. Plaintiff Lacks Standing to Bring California State Law Claims Because it is Not a California Resident.

Plaintiff does not have standing to bring California state law claims because it is not a California resident, and did not suffer the harms it complains about. It cannot bring claims on behalf of its members.

1 Ou
2 sp
3 co
4 St
5 on
6 de
7 oc
8 the
9 Ct
10 att

12

11

1314

15

16 17

18

19 20

2122

2324

2526

2728

Our settled principles regarding specific jurisdiction control this case. In order for a court to exercise specific jurisdiction over a claim, there must be an "affiliation between the forum and the underlying controversy, principally, [an] activity or an occurrence that takes place in the forum State." *Goodyear*, 564 U.S., at 919, 131 S.Ct. 2846 (internal quotation marks and brackets in original omitted). When there is no such connection, specific jurisdiction is lacking regardless of the extent of a defendant's unconnected activities in the State. See *id.*, at 931, n. 6, 131 S.Ct. 2846 ("[E]ven regularly occurring sales of a product in a State do not justify the exercise of jurisdiction over a claim unrelated to those sales"). *Bristol-Myers Squibb Co. v. Superior Court of California, San Francisco County*, 137 S. Ct. 1773, 1781, 198 L. Ed. 2d 395 (2017). When confronted by Judge Hamilton about its improper attempts to stand in the shoes of its customers, Plaintiff conceded in oral argument on December 19, 2018 that it lacked standing to bring claims on behalf of its customers:

"THE COURT: So why isn't the harm suffered in Nevada? Just because there are California clients doesn't transfer their harm to your client's harm.

MR. SMITH: No. Understood, Your Honor."

Exhibit 1 at p. 27:11-14

All of Plaintiff's claims which are California State Law claims, or purport to assert standing on behalf of Plaintiff's customers must be dismissed for lack of standing.

D. Plaintiff's Second Amended Complaint Fails to Specify Web Presence's Conduct Giving Rise to Plaintiff's Claims.

A persistent issue resulting from Plaintiff's failure to comply with Rule 11, Plaintiff's SAC lumps all Defendants together to avoid admitting the inconvenient truth that it has no evidence that the Removal Sites knew about, ratified, or participated in the alleged conspiracy. Plaintiff references multiple or all Defendants, and alleges that they are all doing completely different actions, and yet intends to mislead like "Defendants" court making blanket accusations unauthorized access the by SeekingArrangement.com, use of SA Members' personal identifying information and then extortion of a fee to remove such information from the Extortion Websites is illegal and qualifies as 'any unlawful, unfair or fraudulent business act or practice." SAC ¶ 120. Plaintiff never alleges that Web Presence obtained or reposted any of Plaintiff customers' personal information, or engaged in any actionable

conduct, even though it is difficult to tell from Plaintiff's intentional habit of lumping all Defendants together, and stating multiple separate but distinct actions that each took (e.g. SAC ¶ 117, 120).

Even Judge Hamilton admonished Plaintiff for this practice after reviewing Plaintiff's First Amended Complaint:

"THE COURT: It's difficult to discern from your Complaint because you assert every cause of action against every defendant and you don't differentiate the conduct engaged in by each different defendant, so I have no idea what you're doing here."

Exhibit 1 at p. 34: 11-14.

When a plaintiff fails to specify the claim, it is impossible for a defendant to respond on the merits and the claim must be dismissed. A complaint that offers labels and conclusions, or formulaic recitation of elements of cause of action, does not survive a motion to dismiss. Rule 8(a)(2), Fed.R.Civ.P.; Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). Nor does a "complaint suffice if it tenders naked assertions devoid of further factual enhancement." Id. Plaintiff cannot simply parrot the elements of a cause of action or make conclusory statements that "conduct is unlawful" to survive a motion to dismiss. Plaintiff must allege specific facts. Those facts should describe whatever conduct Web Presence allegedly engaged in that give rise to liability. See id. at 678. Plaintiff does not allege that Web Presence had unauthorized access to SeekingArrangement.com — only "Defendants." Plaintiff does not allege that Web Presence improperly used SA Members' personal identifying information — only "Defendants." To the extent that Plaintiff alleges that Web Presence "extorts" fees from anyone, it has failed to show anything in its complaint but a voluntary customer approaching it about content removal. This is not extortion. For the same reasons that it failed to allege facts sufficient to support claims for tortious interference, Plaintiff fails to allege facts sufficient to support a claim for unfair competition against Web Presence.

Highlighting just one of the many occurrences of this vagueness problem, Plaintiff's statutory unfair competition claims fail with respect to Web Presence because it alleges that "Defendants" violated the Cal. Bus. & Prof. Code § 17200 et seq. by engaging in "any unlawful, unfair or fraudulent business act or

⁴Reflex's claim for unfair competition also fails insofar as Reflex relies on a general allegation that Defendants have engaged in conduct that "qualifies as 'any unlawful, unfair or fraudulent business act or practice'." Failure to specify the specific basis—whether unlawful, unfair, or fraudulent—for a claim of unfair competition under California law is sufficient grounds for dismissal. *See Clark*, 732 F. Supp. 2d at 1050.

1 | F 2 | i 3 | F 4 | t 5 | c

practice." This allegation fails in multiple aspects to state a claim upon which relief can be granted. First, it fails to state what Web Presence did that was an "unlawful, unfair or fraudulent business act or practice." This is yet another occurrence of Plaintiff's practice to make blanket and conclusory allegations that lack the specificity necessary for anyone – Web Presence included – to determine precisely what conduct is complained of.

Plaintiff also fails to specify what portion of Cal. Bus. & Prof. Code § 17200 et seq. Web Presence specifically violated. Cal. Bus. & Prof. Code § 17200 makes unlawful "any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code." Section 17500 contains at least dozens, if not hundreds of various types of prohibited business conduct. *Id.* Plaintiff's deficient pleading makes it impossible for Web Presence to identify which section of the code it allegedly violated, what conduct Web Presence allegedly took in violation of the code, and prevents Web Presence from responding in a meaningful way because nobody can tell what Plaintiff is complaining about. The appropriate remedy is dismissal. *See, In re Carrier IQ, Inc.*, 78 F.Supp.3d 1051, 1098 (N.D. Cal. 2015). Plaintiff's duplicative claim for unfair competition under common law fails for the same reasons.

Plaintiff has failed to allege with any degree of specificity what conduct Web Presence has engaged in that gives rise to liability, or what damages it has suffered. To the extent Plaintiff suffered any damages whatsoever, it has failed to allege how Web Presence is responsible for causing those damages. For the foregoing reasons, Plaintiff's claims must be dismissed as to Web Presence.

III. CONCLUSION.

There is no causal link between Web Presence, any of the other Defendants, and the harm that Plaintiff allegedly suffered. Had Plaintiff bothered to investigate its claims, it would know that it has no jurisdiction over Web Presence and no claims against it. Unfortunately, Plaintiff has forced Web Presence to appear in federal court forcing the burden on it to prove its innocence. *That is not the law*.

Plaintiff may have a case against the Doe defendants. Web Presence believes that the Data Miners may be in league with a content removal provider, but that these entities thought it would be too suspicious to only recommend one provider. The true defendants likely attempted to obfuscate their involvement by placing banner ads on the Extortion Sites for other reputation management providers so

it would not be immediately apparent who was behind the scheme. That would explain why there were advertisements for Web Presence and Marca Global on the Extortion Websites that neither Web Presence nor Marca Global paid for. It would also explain why text messages were being sent that appear to drive traffic to Web Presence even though Web Presence did not send or authorize such messages.

But Plaintiff has clearly made an incorrect inferential leap that those ads and text messages mean that Web Presence and the Data Miners or Does are working together. This is not true, and Plaintiff has no evidence of Web Presence associating with any of the other Defendants. The only conduct that can be attributed to Web Presence is perfectly legal. Plaintiff's conspiracy claims remain vague and nonspecific, even though Web Presence has repeatedly demanded proof of the alleged conspiracy. Clearly there is no such evidence, which is why Plaintiff's conspiracy claims remain vague and non-specific. This is the inherent problem with this case. Plaintiff could attempt to litigate this case for years against Web Presence, and it will never find any evidence against Web Presence because there is nothing for them to find. Plaintiff's stubborn insistence on keeping Web Presence in this case is not supported by facts, nor by law, and is causing Web Presence significant financial harm.

For all the foregoing reasons, Web Presence respectfully requests that the Court dismiss Plaintiff's Second Amended Complaint against it. Plaintiff fails to state a claim against Web Presence, or a claim upon which relief may be granted, and this Court lacks subject matter jurisdiction.

RESPECTFULLY SUBMITTED this 12th day of March, 2019.

21

26

27

28

MAY, POTENZA, BARAN & GILLESPIE, P.C.

By: /s/Michelle Mozdzen

Jean Schwartzer Michelle Mozdzen pro hac vice Christopher B. Ingle pro hac vice Attorneys for Defendant Web Presence, LLC

CERTIFICATE OF SERVICE 1 2 I hereby certify that on March 12, 2019. I electronically filed the foregoing **WEB PRESENCE**, 3 LLC'S MOTION TO DISMISS PLAINTIFF'S SECOND AMENDED COMPLAINT with the 4 Clerk of Court using CM/ECF system which will send notification of such filing to the following e-mail 5 addresses: 6 James D. Boyle, Esq. Sean E. Story, Esq. 7 400 South Fourth Street, Third Floor Las Vegas, Nevada 89101 8 jboyle@nevadafirm.com sstory@nevadafirm.com 9 Attorney for Marca Global, LLC d/b/a www.InternetReputation.com 10 Chad T. Nitta (appearance pro hac vice) 11 KUTAK ROCK LLP 1801 California St. Suite 300 12 Denver, CO 80202 Tel: (303) 297-2400 13 chad.nitta@kutakrock.com blair.kanis@kutakrock.com 14 Attorney for Marca Global, LLC d/b/a www.InternetReputation.com 15 Joseph A.Schaeffer, Esq. 16 SMITH WASHBURN, LLP 500 South Grand Avenue, Suite 1450 17 Los Angeles, California 90071 Attorney for Plaintiff Reflex Media, Inc. 18 Mark L Smith 19 Jacob L. Fonnesbeck SMITH WASHBURN, LLP 20 6871 Eastern Avenue, Suite 101 Las Vegas, Nevada 89119 21 msmith@smithwashburn.com ifonnesbeck@smithwashburn.com 22 Attorney for Plaintiff Reflex Media, Inc. 23 By:/s/ *Michelle Mozdzen* 24 25 26 27

28